Atty. Dkt. No. 061602-2675

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant: LEMILAINEN et al.

Title: SIM BASED AUTHENTICATION AS PAYMENT METHOD IN PUBLIC ISP ACCESS NETWORKS

Appl. No.: 09/303424

Filing Date: May 3, 1999

Examiner: Abdi, Kambiz

Art Unit: 3621

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450**, on the date below.

LAURA MARKHAM
(Printed Name)

Laura Markham
(Signature)

5-24-06
(Date of Deposit)

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Under the provisions of 37 C.F.R. § 41.37, this Appeal Brief is being filed together with a credit card payment form covering the $500.00 37 C.F.R. 41.20(b)(2) appeal fee. If this fee is deemed to be insufficient, authorization is hereby given to charge any deficiency (or credit any balance) to the undersigned deposit account 06-1450.

REAL PARTY IN INTEREST

The real party in interest in this Appeal is Nokia Corporation of Espoo, Finland. This interest is evidenced by an assignment from the inventor to Nokia Corporation, which is recorded at Reel 010262, Frame 0708.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences that will directly affect, be directly affected by, or have a bearing on the present appeal, that are known to Appellant or Appellant's patent representative.

STATUS OF CLAIMS

Claims 1-35 were pending in the application when a final Office Action dated June 30, 2005 was issued. In the June 30, 2005 final Office Action, each of claims 1-35 were rejected. The Examiner's rejection of claims 1-35 are being appealed.

Claims 1-3, 5-10, 13-15, 17, 18, 21-30, 32, 34, and 35 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,577,643 (Rai et al.), and U.S. Patent No. 6,036,090 (Rahman et al.), and further in view of U.S. Patent No. 5,729,537 (Billstrom).

Claims 4, 11, 12, 16, 19, 20, and 31-33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,577,643 (Rai et al.), in view of U.S. Patent No. 6,036,090 (Rahman et al.), in view of U.S. Patent No. 5,729,537 (Billstrom), and further in view of U.S. Patent No. 5,930,777 (Barber).

The claims in their current condition are attached hereto in the Appendix.

STATUS OF AMENDMENTS

No claims have been amended in the present application subsequent to the receipt of the final Office Action dated June 30, 2005.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention relates to a system and method for charging a user for obtaining access to a packet data network. (FIGS. 1, 2, page. 1, lines 7-9). The present invention utilizes a series of communications between a user 12, a security server 24 of a network that provides billing for communications by the user 12 through a first network, a public security server 26, and an access server 30 of a second network 16 through which connectivity between the user 12 and the packet data network 14 is effected. (FIG. 1, page. 3, lines 14 - 23, page. 7, line 23 - page. 8, line 4). The first series of communications are characterized as purchase communications in which the user 12 inputs a user request (step 1) to the first network 10 which requests that the user 12 be authorized for connection to the packet data network 14 through the second network 16 for a specified quantity "n" of communications, which are referred hereinafter as "service units". (FIG. 1, page 3, line 23 – page 4, line 2, page 9, lines 1-4). Service units without limitation may be in terms of a specified time of connection of the user through the second network 16 to the packet data network 14 or, alternatively, for a fixed monetary value which provides a variable quantity of connection time to the packet data network 14 depending upon a rate structure which varies depending upon the time of connection or other factors. (FIG. 1, page 4, lines 2-9). The n service units are used to provide authority for and quantity of connection to the packet data network 14 through the second network 16 which, in a preferred application, provides connectivity to the packet data network 14 when the user 12 is roaming in the second network 16. (FIG. 1, page. 8, line 25 – page. 9, line 13, Abstract). The user's home security server 24 then transmits to the public security server 26 of the second network the user request (step 2) and an authorization of payment by the first network 10 to the second network 16 for the user's use of the packet data network 14 through the second network 16. (FIG. 1, page. 4, lines 9-13, page. 9, line 14 - page 10, line 2) Furthermore, the public security server 26 calculates the n service units and stores them for future consumption. (page 10, line 2-page. 11, line 6, Abstract). Thereafter, the second network 16 transmits to the first network 10 authentication information (step 3) granting user authentication to the user 12 to obtain connection through the second network 16 to the packet data network 14. (FIG. 1, page 4, lines 13-20, page. 11, lines 7-21) Calculation of the authentication information by the second network 16 is performed by a resident Subscriber Identification Module (SIM) which performs a calculation analogous to the SIM in the GSM system. (page 5, lines 4-8) Furthermore, the authentication information is in the form of n information triplets, each corresponding to information necessary to encode an individual service unit, each triplet preferably including an individual RAND, a signed response (RES), and a cipher key Kc. (FIG. 1, page 11, lines 12-21). The authentication information is the transmitted from the first network 10 to the user 12 (step 4), which informs the user 12 that authentication to obtain a connection to the packet data network 14 has been obtained. (FIG. 1, P. 4, line 20 – page. 5, line 8, page. 11, line 22-page. 12, line 7, Abstract).

The inputting of the user request (step 1) to the first network 10, the transmitting of the user request and authorization of payment to the second network 16 (step 2) and the transmitting of the authentication information from the second network 16 to the first network 10 (step 3) and transmitting of the authentication information from the first network 10 to the user 12 (step 4) can be by secured communications. (FIG. 1, page 5, lines 9-14) Therefore, the transmitting of the shared secret key Kc is not open to the public and furthermore, it is not necessary, as with GSM communications, for the user's mobile device to contain the algorithms to compute the shared secret key Kc in order for subsequent communications between the user 12 and the packet data network 14 for secured communications to be established between a user 12 and the packet data network 14. (FIG. 1, page. 5, lines 14–21, page. 12, lines 8–26).

The consumption of the authorized service units occurs after the user 12 has been informed that access to the packet data network 14 has been granted and is initiated by the user 12 transmitting to the second network 16, such as, but not limited to, during roaming, at least one request (step 1) for consumption of at least one service unit comprising a RAND and a SRES. (FIG. 2, page. 5, line 22 – P. 6, line 1, page. 13, lines 1-24). The second network 16 compares the RAND and SRES of each request for consumption of at least one service unit received from the user 12 with stored RANDs and SRESs to determine if a match exists in step 2. (FIG. 2, page. 6, lines 1–5, page. 13, line 25 – page. 14, line 5). If a match exists, the second network 16 permits data packets to pass through the second network 16 between the user 12 and the packet data network 14 (step 3). (FIG. 2, page 6, lines 5-7, page 13, line 27- page 14, line 5, page 15, lines 6-17) The second network 16 debits from a stored value of n service units which have been granted to the user 12 a number of consumed service units which are identified in each request for consumption of at least one service unit the number of consumed service units equals the number of n granted service units. (FIG. 2, page 6, lines 8-13, page 14, lines 11-19). In a preferred application, each unused service unit is stored in the second network 16 in a first list and each used service unit is stored in the second network 16 in a second list. (FIG. 2, page 6, lines 13-16, page 14, line 12 – page 15, line 1). Preferably, the first and second lists are hash tables which avoid potential collisions of service units. (page 6, lines 16-17). This allows a user 12 to utilize packet data network 14 through a second network 16 without having any roaming agreement or contract between a first network 10 and either the packet data network 14 or the second network 16. (FIGS. 1 and 2, page 1, line 12-page 2, line 2, page 3, lines 14-23).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The first ground of rejection to be reviewed on appeal is the Examiner's rejection of Claims 1-3, 5-10, 13-15, 17, 18, 21-30, 32, 34, and 35 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,577,643 (Rai et al.), and U.S. Patent No. 6,036,090 (Rahman et al.), and further in view of U.S. Patent No. 5,729,537 (Billstrom).

The second ground of rejection to be reviewed on appeal is the Examiner's rejection of Claims 4, 11, 12, 16, 19, 20, and 31-33 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,577,643 (Rai et al.), in view of U.S. Patent No. 6,036,090 (Rahman et al.), and U.S. Patent No. 5,729,537 (Billstrom), and further in view of U.S. Patent No. 5,930,777 (Barber).

The claims in their current condition are attached hereto in the Appendix.

ARGUMENT

I. The Rai et al. reference, the Rahman et al. reference, and the Billstrom reference do not render obvious Claims 1-3, 5-10, 13-15, 17, 18, 21-30, 32, 34, and 35 of the present invention because the references do not disclose, teach, or suggest obtaining a connection by a user through a first network and through a second network to a packet data network with the connection being paid for by the first network making payment to the second network, wherein the user is anonymous and there is no roaming agreement or contract with the packet data network for the user to obtain the connection thereto, as well as the resulting benefits.

The Examiner has not made an adequate showing that claims 1-3, 5-10, 13-15, 17, 18, 21-30, 32, 34, and 35 are rendered obvious by U.S. Patent No. 6,577,643 (Rai et al.), in view of U.S. Patent No. 6,036,090 (Rahman et al.), and further in view of U.S. Patent No. 5,729,537 (Billstrom). More particularly, regarding claims 1, 21, 26, and 27, the Examiner has failed to cite any reference or any combination of references that teach a method of obtaining connection by a user through a first network and through a second network to a packet data network, the connection to the packet data network being effected through the second network, with the connection being paid for by the first network making payment to the second network. Furthermore, the Examiner has failed to cite any reference or any combination of references that teach a payment method, wherein a requirement for the payment is the result of communications which first originate with the user request to the first network, and wherein the user is anonymous and there is no roaming agreement or contract with the packet data network.

In *In re Rijckaert*, 9 F.3d 1531, 1532, (Fed. Cir. 1993), the Federal Circuit outlined the burden on the PTO as follows:

> In rejecting claims under 35 U.S.C. 103, the examiner bears the initial burden of presenting a *prima facie* case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. *Id.* "A *prima facie* case of obviousness is established when the teachings from the prior art itself would appear to have suggested the claimed subject matter to a person of ordinary skill in the art." *In re Bell*, 991 F.2d 781, 782, 26 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1993) (quoting *In re Rinehart*, 531 F.2d 1048, 1051, 189 U.S.P.Q. 143, 147 (CCPA 1976)). If the examiner fails to establish a *prima facie* case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988).

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some reasonable suggestion or motivation to modify the prior art reference or to combine reference teachings. Second, there must be a reasonable expectation of success of achieving the desired goals. Finally, the prior art references when combined must teach all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on the Applicant's disclosure. *In re Vaeck*, 947 F.2d 488 (Fed. Cir. 1991).

In this instance, this test is not met. Rai et al. does not teach all the claim limitations of independent claims 1, 21, 26, and 27. Rai et al. teaches that when a roaming end system 60 has traveled to a location where foreign wireless service provider 62 provides service, the end system 60 requests authorization to use the foreign service provider's service, which includes accessing Internet service provider's network 74. Furthermore, Rai et al. teaches that the end system 60 would first have to request authorization from the foreign wireless service provider 62, after which a serving interworking function (IWF) 66 communicates with a home

IWF 72 to effect authentication and registration. (*See* e.g., FIG. 3, column 6, line 64 – column 8, line 61 of Rai et al.) In Section 7 of the office action dated June 30, 2005, the Examiner read the home wireless service provider 70 (*See* FIG. 3 of Rai et al.) as the claimed first network and the foreign wireless service provider 62 (*See* FIG. 3 of Rai et al.) as the claimed second network. Claims 1, 21, 26, and 27, however, describe requesting access to a packet data network and requesting that payment be made by the first network to the second network first as originating from communications from a user to a first network. Therefore, assuming arguendo that the Examiner's interpretation of the providers 62 and 70 is correct, Rai et al. in fact teaches the reverse of what is described in claims 1, 21, 26, and 27, i.e., that the user would communicate first with the second network.

In addition to the above, Rai et al. requires that the connection from the end system 60 to ISP network 74 is made through the home wireless service provider 70 and subsequently through the foreign wireless service provider 62. However, claims 1, 21, 26, and 27 require that a user is authorized for connection to the packet data network through only the second network. Once the end user has roamed to the second network and has connected to the packet data network through the second network, no communications are effected between the first user and the first network. (*See* FIG. 2). The only time the user communicates with the first network is before the user has roamed into the second network and is requesting authorization. (*See* FIG. 1).

Even if one were to interpret the foreign wireless service provider 62 of Rai et al. as the claimed first network and the home wireless service provider 70 of Rai et al. as the claimed second network, claims 1, 21, 26, and 27 still patentably define over Rai et al. because this interpretation would mean that the foreign wireless service provider 62 would be the network paying the home wireless service provider 70. This is clearly not the case, as there is no reason why a foreign service provider would pay a home service provider for an end system that is roaming on the foreign service provider's network.

Furthermore, Rai et al. does not teach that the end system 60 is anonymous, nor does it teach that there is no roaming agreement or contract with the packet data network. In fact, Rai et al. repeatedly states that the home wireless service provider 70 and the foreign wireless service provider 62 must have a roaming or service agreement.

> "Using this feature, end systems are able to roam away from the home network to a foreign network and still get service, provided of course that the foreign wireless service provider and the end system's home wireless service provider have a service agreement." (*See* column 8, lines 41 – 47 of Rai et al.).

In addition, the ISP network 74 is either a part of the home wireless service provider network 70 or the home wireless service provider 70 subscribes to ISP network 74 as demonstrated below.

> "Here it is assumed that both end systems have subscribed to the same ISP." (*See* column 15, lines 42–44 of Rai et al.).

> "In order for this configuration to work, not only must there be roaming agreements between the home and the foreign wireless service providers, but there also must be agreements between the foreign wireless service provider and the end system's internet service provider directly or through an intermediary." (*See* column 16, lines 26 – 31 of Rai et al.).

Rai et al. also does not teach all the claim limitations of claims 22 – 25[1]. In Section 7 of the office action dated June 30, 2005, the Examiner interprets Rai et al. as teaching that a second network debits from a stored value of service units which have been granted to the user a number of consumed service units. However, no mention nor suggestion of the use of service units is made in the portions of Rai et al. cited by the Examiner. Column 6, lines 26–35 of Rai et al., for example, generally discuss collecting accounting data and the interfaces supported by an accounting server used to collect the accounting data. Column 27, line 44–column 30, line 46 of Rai et al. also generally discuss standard accounting methods where accounting data is collected by a serving IWF 66 and by a home IWF 72. Rai et al. merely teaches that the start and end of a user's roaming session is marked, and a home IWF 72 and a serving IWF 66 exchange records and accounting data so that records can later be audited and settled, including the marked sessions. In other words, the foreign wireless service provider 62 keeps track of the time spent by the end system 60 in the foreign wireless service provider's network and sends this "bill" to the end system 60's home wireless network provider 70.

By contrast, claims 22-25 describe using specific service units, of which a certain number are purchased and stored, and are debited according to a user's use of the packet data network. Claim 22, for example, recites:

> ...after the user is informed that authentication to obtain connection to the packet data network has been obtained, the user transmits to the second network at least one request for consumption of at least one service unit and the second network

[1] The Examiner rejected claims 22 – 25 with claims 1, 21, 26, and 27. However, claims 1, 21, 26, and 27, do not recite any limitation regarding the use of service units. Therefore, claims 22 – 25 which do recite limitations regarding the use of service units have been addressed separately.

> debits from a stored value of service units which are granted to the user a consumed number of service units

Even though service units can be defined in terms of a specified time of connection, they are a discrete entity used in a wholly different way than a foreign wireless service provider merely recording a start and end time of a user's session and later billing the home wireless provider of that user. In fact, the Examiner admitted in Section 19 of the June 30, 2005 office action that Rai et al. merely teaches accounting aspects in general and not any actual debiting as claimed in the present invention.

Furthermore, neither Rahman et al. nor Billstrom cure the deficiencies of Rai et al. With regard to Rahman et al., the Examiner asserted that:

> As the visited network communicated with the home network of the user and request payment and start charging the home network for the communication services provided by the second network to the user (free roamer) based on the pre-assigned amount of funds for the use by the users home network (balance) as well as there is no agreement or contract. (*See* Section 7, page 4 of the office action dated June 30, 2005).

However, Appellant respectfully disagrees with the Examiner's interpretation of Rahman et al. Rahman et al. in fact merely teaches that a user can pre-program a mobile terminal (MT) 24 with a credit card or debit card number. Once MT 24 enters a visited area 26, it sends a registration request to the appropriate network elements. The appropriate network elements then forward the credit card or debit card information to a prepayment clearing house 38 which decides whether or not the information allows MT 24 access to visited area 26. In Rahman et al., there is no interaction with a first or home network whatsoever because the prepayment clearing house 38 is simply a standard credit card authorization entity independent of any communications network. (*See* FIG. 2, column 3, line 49 – column 4, line 53 of Rahman et al.). Even if the prepayment clearing house 38 resides in a home area, this arrangement would only be effective for a user requesting access to the communications services provided by visited area 26, not a third packet data network, as is the case in claims 22 and 24. Therefore, Rahman et al. cannot cure the deficiencies of Rai et al.

Billstrom also fails to cure the deficiencies of either Rai et al. or Rahman et al. Billstrom is drawn to a system and method for providing anonymous communications. However, like Rahman et al. discussed above, Billstrom is only concerned with, at best, two networks, and operates by assigning a group identifier to all mobile stations 12 that are a part of that group. Therefore, the specific identity of any one mobile subscriber 12 is hidden, with access to an external data network 108 being given pursuant to the group identifier (IMGI) instead of a mobile subscriber identifier (IMSI) unique to each mobile subscriber 12. (*See*, e.g., column 5, lines 9–34, column 5, line 66 – column 6, line 10, column 7, line 17 – column 8, line 54). Therefore, the method of achieving anonymity is completely different from claims 1, 21, 22, 24, and 26, which provide anonymity by virtue of the fact that the user only requests authorization from the first network, and it is the second network that generates and transmits the authentication information required for authorization . Moreover, in Billstrom, some type of roaming agreement or restrictive contract is required. Billstrom requires that Internet Protocol (IP) addresses of any entity that will be communicating on a network are known beforehand. It is simply that in Billstrom, the address is one that is associated with a group. (*See* column 10, lines 34–45, column 11, lines 28–33). Therefore, even though Billstrom does teach anonymous roaming, it does not cure all the deficiencies already discussed above regarding Rai et al. and Rahman et al.

Lastly, none of the prior art references cited by the Examiner, alone or in combination, are believed to read on claims 2, 3, 5–10, 1 –15, 17, 18, 28,30, 32, 34, and 35, at least due to their dependence on claims 1, 21, 22, 24, and 26

Because many of the limitations of claims 1–3, 5–10, 13-15, 17, 18, 21–30, 32, 34, and 35 cannot be found in any of the prior art references cited by the Examiner, the only reasonable conclusion is that the rejection of these claims under 35 U.S.C. § 103(a) is improper.

II. The Rai et al reference, the Rahman et al. reference, the Billstrom reference, the Barber reference, and the Kirby reference do not render obvious Claims 4, 11, 12, 16, 19, 20, and 31 – 33 of the present application because the references do not disclose, teach, or suggest obtaining a connection by a user through a first network and through a second network to a packet data network with the connection being paid for by the first network making payment to the second network, wherein the user is anonymous and there is no roaming agreement or contract with the packet data network for the user to obtain the connection thereto, as well as the resulting benefits.

The Examiner has not made an adequate showing that claims 4, 11, 12, 16, 19, 20, and 31-33 are rendered obvious by U.S. Patent No. 6,577,643 (Rai et al.), in view of U.S. Patent No. 6,036,090 (Rahman et al.), and U.S. Patent No. 5,729,537 (Billstrom), in view of U.S. Patent No. 5,930,777 (Barber)[2]. More particularly, regarding claims 4, 31, and 33, the Examiner has failed to cite any reference or any combination of references that teach a method of obtaining connection by a user through a first network and through a second network to a packet data

[2] In the body of the rejection, Section 15, the Examiner discusses a Kirby reference although it has not been listed as one of the applied prior art references. In reviewing the case history, it appears that U.S. Patent No. 6,047,179 (Kirby) was cited and applied in an office action dated September 10, 2004. Appellant assumes the Examiner is referring to this reference and merely forgot to cite it in the outstanding office action.

network, the connection to the packet data network being effected through the second network, with the connection being paid for by the first network making payment to the second network. Furthermore, the Examiner has failed to cite any reference or any combination of references that teach a payment method, wherein a requirement for the payment is the result of communications which first originate with the user request to the first network, and wherein the user is anonymous and there is no roaming agreement or contract with the packet data network.

Like claim 3 discussed previously, claims 4, 31, and 33 require the use of a service unit. However, and as already discussed above, Rai et al. does not teach the use of service units. Moreover, the cited portions of Rai et al. in Section 15 of the office action dated June 30, 2005 also do not teach encoding each service unit with a different random number. Nowhere in column 26, lines 4–10 or column 30, lines 45–56 of Rai et al. is random number encoding of a service unit taught. These cited portions merely generally discuss accounting packets and shared secrets.[3]

With regard to Kirby, although a debiting service may be taught, at best only two networks are contemplated, not three as in claims 1, 21, 22, 24, and 26. This is shown in FIGS. 1 and 3–5 of Kirby. Moreover, although Kirby uses the term "debit unit," this debit unit refers to an actual cellular telephone or similar device using a prepaid telecommunications service which is old and well known in the relevant art. (*See*, e.g., column 10, lines 46–55, column 11, line 48 – column 12, line 39). This debit unit taught by Kirby is not analogous to the claimed service

[3] Even though the Examiner has argued that Rai et al. teaches random number encoding of service units, the Examiner stated immediately afterwards in the June 30, 2005 office action that Rai et al. does not in fact explicitly disclose that each service unit has a different random number and applies the Barber and Kirby references.

unit, which as already discussed above, refers not to a physical device, but to a specified quantity of communications. This is clearly discussed at page 3, line 23 – page. 4, line 2 of the specification. Moreover, Kirby teaches the same standard pre-paid service method as in Rahman et al., in that a debit unit 80c must already be registered in a visited network 60 in order for it to receive service. Therefore, some roaming agreement or contract is still needed, which is not the case with the present invention.

As to Barber, the Examiner referred to column 30, lines 45–56 to show different random number encoding of each service unit. However, no column 30 exists in the Barber reference.[4] Regardless, Barber does not cure the deficiencies of any of the previously discussed prior art. Barber is drawn to a method for charging a consumer for access over a single network to a vendor's information based upon a third party which is referred to as a banker. (*See*, e.g., column 5, lines 6–23, Abstract). Clearly, the banker is not a second network and is in essence merely an entity which mints tokens which permit the purchasing of access to a vendor-particular Web Page via the Internet or similar network. As Barber clearly does not teach the use of service units let alone encoding each service unit with a different random number, it does not cure the deficiencies of any of the above-discussed prior art references.

In addition, none of the prior art references cited by the Examiner, alone or in combination, are believed to read on claims 11, 12, 16, 19, and 20, for the reason that they depend from claims 1, 21, 22, 24, and 26. Moreover, in rejecting claims 19 and 20 in Section 19

[4] It is believed that the Examiner in fact was referring to column 30, lines 45-56 of Rai et al., as this portion of Rai et al. was repeatedly cited in the June 30, 2005 office action. However, as already discussed above, Rai et al. does not teach the claimed limitation.

of the outstanding office action, for example, although the Examiner states that Barber teaches certain claimed limitations, reference is made to Rai et al., which as already discussed above, fails to teach all the limitations of the present invention, including the use of service units and the use of hash tables.

Because these limitations cannot be found in any of the prior art references cited by the Examiner, the only reasonable conclusion is that the rejection of claims 4, 11, 12, 16, 19, 20, and 31-33 under 35 U.S.C. § 103(a) is improper. Furthermore, because dependent claims 4, 11, 12, 16, 19, 20, and 31-33 are each directly or indirectly dependent upon independent claims 1, 21, 22, 24, and 26, Appellant submits that each of these claims are allowable for at least the same reasons as discussed above.

III. Conclusion

Claims 1-3, 5-10, 13-15, 17, 18, 21-30, 32, 34, and 35 would not have been obvious to a person of ordinary skill in the art, at the time the invention was made based upon U.S. Patent No. 6,577,643 (Rai et al.), in view of U.S. Patent No. 6,036,090 (Rahman et al.), and further in view of U.S. Patent No. 5,729,537 (Billstrom). Claims 4, 11, 12, 16, 19, 20, and 31-33 also would not have been obvious to a person of ordinary skill in the art, at the time the invention was made based upon U.S. Patent No. 6,577,643 (Rai et al.), in view of U.S. Patent No. 6,036,090 (Rahman et al.), and U.S. Patent No. 5,729,537 (Billstrom), and U.S. Patent No. 5,930,777 (Barber), and further in view of U.S. Patent No. 6,047,179 (Kirby). Accordingly, favorable consideration and allowance of the application is respectfully requested.

CLAIMS APPENDIX

1. A method of obtaining connection by a user through a first network and through a second network to a packet data network with the connection being paid for by the first network making payment to the second network comprising:

inputting a user request to the first network which requests that the user be authorized for connection to the packet data network through the second network;

transmitting from the first network to the second network the user request and an authorization of payment to the second network by the first network for the use by the user of the packet data network;

transmitting from the second network to the first network authentication information granting the user authentication to obtain connection through the second network to the packet data network; and

transmitting the authentication information from the first network to the user which informs the user that authentication to obtain connection to the packet data network has been obtained; and wherein

a requirement for the payment to be made for the connection to the packet data network is the result of communications which first originate with the user request to the first network, the user is anonymous and there is no roaming agreement or contract with the packet data network for the user to obtain the connection thereto.

2. A method in accordance with claim 1 wherein:

the user request includes a quantification of connectivity which the user requests to the packet data network.

3. A method in accordance with claim 2 wherein:

the quantification comprises at least one service unit with each service unit being encoded with a random number.

4. A method in accordance with claim 3 wherein:

each service unit is encoded with a different random number.

5. A method in accordance with claim 1 wherein:

the authentication information comprises a shared key which may be used to create secure communications between the user and the packet data network.

6. A method in accordance with claim 5 wherein:

authentication information is a subscriber identification module SIM comprising a number n of service units with each service unit comprising a different random access number uniquely identifying each service unit, a signed response SRES and the shared key Kc.

7. A method in accordance with claim 2 wherein:

the authentication information comprises a shared key which may be used to create secure communications between the user and the packet data network.

8. A method in accordance with claim 7 wherein:

authentication information is a subscriber identification module SIM comprising a number n of service units with each service unit comprising a different random access number uniquely identifying each service unit, a signed response SIRES and the shared key Kc.

9. A method in accordance with claim 3 wherein:

the authentication information comprises a shared key which may be used to create secure communications between the user and the packet data network.

10. A method in accordance with claim 5 wherein:

the second network computes a subscriber identification module SIM comprising the number of service units with each service unit comprising a different random access number uniquely identifying each service unit, a signed response and the shared key Kc.

11. A method in accordance with claim 4 wherein:

the authentication information comprises a shared key which may be used to create secure communications between the user and the packet data network.

12. A method in accordance with claim 11 wherein:

authentication information is a subscriber identification module SIM comprising the number of service units with each service comprising a different random access number uniquely identify each service unit, a signed response and the shared key.

13. A method in accordance with claim 1 wherein:

the inputting of the user request to the first network, the transmitting of the user request and an authorization of payment to the second network, and the transmitting of the authentication information from the second network to the first network and to the user are by secure communications.

14. A method in accordance with claim 2 wherein:

the inputting of the user request to the first network, the transmitting of the user request and an authorization of payment to the second network, and the transmitting of the authentication information from the second network to the first network and to the user are by secure communications.

15. A method in accordance with claim 3 wherein:

the inputting of the user request to the first network, the transmitting of the user request and an authorization of payment to the second network, and the transmitting of the authentication information from the second network to the first network and to the user are by secure communications.

16. A method in accordance with claim 4 wherein:

the inputting of the user request to the first network, the transmitting of the user request and an authorization of payment to the second network, and the transmitting of the authentication information from the second network to the first network and to the user are by secure communications.

17. A method in accordance with claim 5 wherein:

the inputting of the user request to the first network, the transmitting of the user request and an authorization of payment to the second network, and the transmitting of the authentication information from the second network to the first network and to the user are by secure communications.

18. A method in accordance with claim 3 wherein:

after the user is informed that authentication to obtain connection to the packet data network has been obtained, the user transmits to the second network at least one request for consumption of at least one service unit comprising a random number RAND and a signed response SRES;

the second network compares the random number RAND and signed response SIRES of each request for consumption of at least one service unit received from the user with stored random numbers RAND and signed responses SIRES to determine if a match exists; and if a match exists, the second network permits data packets to pass . through the second network between the user and the packet network.

19. A method in accordance with claim 18 wherein:

the second network debits from a stored value of service units which have been granted to the user a number of consumed service units which are identified in each request for consumption of at least one service unit until the number of consumed service units equals the number of granted service units.

20. A method in accordance with claim 19 wherein:

each unused service unit is stored in the second network in a hash table and each used service unit is stored in the second network in a hash table .

21. A system comprising:

a user;

a first network which is connectable to the user;

a second network which is connectable to the first network and to the user; and

a packet data network which is connectable to the second network; and wherein

the first network, in response to a user request to the first network that the user be authorized for connection to the packet data network through the second network with the connection being paid for by the first network making payment to the second network, transmits to the second network the user request and an authorization of payment by the first network for the use by the user of the packet data network, the second network transmits to the first network authentication information granting the user authentication to obtain connection through the second network to the packet data network, and the first network transmits to the user authentication information which informs the user that authentication to obtain connection to the packet data network has been obtained ; and wherein

a requirement for the payment to be made is the result of communications which first originate with the user request to the first network, the user is anonymous and there is no roaming agreement or contract with the packet data network for the user to obtain the connection thereto.

22. A method of obtaining connection by a user through a first network and through a second network to a packet data network with the connection being paid for by the first network making payment to the second network comprising:

inputting a user request to the first network which requests that the user be authorized for connection to the packet data network through the second network;

transmitting from the first network to the second network the user request and an authorization of the payment to the second network by the first network for the use by the user of the packet data network;

transmitting from the second network to the first network authentication information granting the user authentication to obtain connection through the second network to the packet data network;

transmitting the authentication information from the first network to the user which informs the user that authentication to obtain connection to the packet data network has been obtained; and

after the user is informed that authentication to obtain connection to the packet data network has been obtained, the user transmits to the second network at least one request for consumption of at least one service unit and the second network debits from a stored value of service units which are granted to the user a consumed number of service units ; and wherein a requirement for the payment to be made for the connection to the packet data network is the result of communications which first originate with the user request to the first network . the user is anonymous and there is no roaming agreement or contract with the packet data network for the user to obtain the connection thereto.

23. A method in accordance with claim 22 wherein:

the number of consumed service units are identified in each request for consumption of at least one service unit until the number of consumed service units equals a number of granted units.

24. A system comprising:

a user;

a first network which is connectable to the user;

a second network which is connectable to the first network and to the user; and

a packet data network which is connectable to the second network; and wherein

the first network, in response to a user request to the first network that the user be authorized for connection to the packet data network through the second network with the connection being paid for by the first network making payment to the second network, transmits to the second network the user request and an authorization of the payment by the first network for the use by the user of the packet data network, the second network transmits to the first network authentication information granting the user authentication to obtain connection through the second network to the packet data network, and the first network transmits to the user authentication information which informs the user that authentication to obtain connection to the packet data network has been obtained; and after the user is informed that authentication to obtain connection to the packet data network has been obtained, the user transmits to the second network at least one request for consumption of at least one service unit and the second network debits from a stored value of service units which are granted to the user a consumed number of service units ; and wherein a requirement for the payment to be made for the connection to the packet data network is the result of communications which first originate with the user request to the first network, the user is anonymous and there is no roaming agreement or contract with the packet data network for the user to obtain the connection thereto.

25. A system in accordance with claim 24 wherein:

the number of consumed service units are identified in each request for consumption of at least one service unit until the number of consumed service units equals a number of granted units.

26. A method of obtaining connection by a user through a first network and through a second network to a packet data network with the connection being paid for by the first network making payment to the second network comprising:

connection to the packet data network through the second network;

transmitting from the first network to the second network the user request and an authorization of the payment to the second network by the first network for the use by the user of the packet data network;

transmitting from the second network to the first network authentication information granting the user authentication to obtain connection through the second network to the packet data network;

transmitting the authentication information from the first network to the user which informs the user that authentication to obtain connection to the packet data network has been obtained;

the user roams to the second network ; the user requests connection to the packet data network while roaming in the second network; and

the second network grants connection to the packet data network while roaming in the second network based upon the authorization of payment received by the second network; and wherein

a requirement for the payment to be made for the connection to the packet data network is the result of communications which first originate with the user request to the first network , the user is anonymous and there is no roaming agreement or contract with the packet data network for the user to obtain the connection thereto.

27. A method in accordance with claim 26, wherein:

the authorization of payment quantifies an amount of payment that the first network will pay to the second network for connection of the user to the packet data network when the user roams in the second network; and

payment for the connection of the user while roaming in the second network for connection to the packet data network is charged against the authorization.

28. A method in accordance with claim 26 wherein:

the authentication information comprises a shared key which may be used to create secure communications between the user and the packet data network.

29. A method in accordance with claim 28 wherein:

the authentication information is a subscriber identification module SIM comprising a number n of service units with each service unit comprising a different random access number uniquely identifying each service unit, a signed response SIRES and the shared key Kc.

30. A method in accordance with claim 26 wherein:

the user request includes a quantification of connectivity which the user requests to the packet data network; and

the quantification comprises at least one service unit with each service unit being encoded with a random number.

31. A method in accordance with claim 30 wherein:

each service unit is encodèd with a different random number .

32. A method in accordance with claim 27 wherein: the user request includes a quantification of connectivity which the user requests to the packet data network; and the quantification comprises at least one service unit with each service unit being encoded with a random number.

33. A method in accordance with claim 3 2 wherein : each service unit is encoded with a different random number.

34. A method in accordance with claim 26 wherein :

after the user is informed that authentication to obtain connection to the packet data network has been obtained, the user transmits to the second network at least one request for consumption of at least one service unit comprising a random number RAND and a signed response SRES;

the second network compares the random number RAND and signed response SRES of each request for consumption of at least one service unit received from the user with stored random numbers RAND and signed responses SRES to determine if a match exists; and

if a match exists, the second network permits data packets to pass through the second network between the user and the packet network .

35. A method in accordance with claim 27 wherein:

after the user is informed that authentication to obtain connection to the packet data network has been obtained, the user transmits to the second network at least one request for consumption of at least one service unit comprising a random number RAND and a signed response SIRES;

the second network compares the random number RAND and signed response SIRES of each request for consumption of at least one service unit received from the user with stored random numbers RAND and signed responses SRES to determine if a match exists; and

if a match exists, the second network permits data packets to pass through the second network between the user and the packet network.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.

Respectfully submitted,

Date MAY 24, 2006

By

FOLEY & LARDNER LLP
Customer Number: 27433
Telephone: (312) 832-4553
Facsimile: (312) 832-4700

G. Peter Albert, Jr.
Attorney for Applicant
Registration No. 37,268